

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	CRIMINAL NO. 15-171
	:	
KEONNA THOMAS,	:	
a/k/a "Fatayat Al Khilafah,"	:	
a/k/a "YoungLioness"	:	

ORDER

AND NOW, this day of , 2016, upon
consideration of the Defendant's Motion for Notice and Discovery of Surveillance Used in the
Government's Investigation of the Defendant and the government's response thereto, it is hereby
ORDERED AND DECREED that the motion is DENIED.

BY THE COURT:

HONORABLE MICHAEL M. BAYLSON
Judge, United States District Court

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA

:

v.

:

CRIMINAL NO. 15-171

**KEONNA THOMAS,
a/k/a "Fatayat Al Khilafah,"
a/k/a "YoungLioness"**

:

:

**GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S
MOTION FOR NOTICE AND DISCOVERY OF SURVEILLANCE USED
IN THE GOVERNMENT'S INVESTIGATION OF THE DEFENDANT**

The United States of America, by its counsel Zane David Memeger, the United States Attorney for the Eastern District of Pennsylvania, Jennifer Arbittier Williams, Assistant United States Attorney for that district, and Paul Casey, Trial Attorney for the Department of Justice, Counterterrorism Section, hereby files its Response in Opposition to Defendant's Motion for Notice and Discovery of Surveillance Used in the Government's Investigation of the Defendant.

A. Background

On April 23, 2015, a grand jury sitting in the Eastern District of Pennsylvania returned an indictment charging defendant Keonna Thomas with attempting to provide material support and resources, "including THOMAS herself as personnel, to a foreign terrorist organization, to wit: the Islamic State of Iraq and the Levant" (ISIL), in violation of 18 U.S.C. § 2339B. Since that time, the government has provided the defense with complete discovery, including all grand jury testimony and exhibits, documents subpoenaed from third-parties, search warrant affidavits and returns of the defendant's social media and email accounts, home, and hard drives, photographs taken during execution of the search warrant at her home, and an audio

recording of the defendant attempting to purchase a quick flight out of the country (after the government seized her hard drives).

In addition to producing voluminous unclassified discovery in this case, the government filed an *ex parte*, sealed, classified motion for a protective order pursuant to Section 4 of the Classified Information Procedures Act (CIPA). Section 4 of CIPA authorizes a court “upon a sufficient showing” to deny or otherwise restrict discovery by the defendant of classified documents and information belonging to the United States.¹ 18 U.S.C. App. III § 4; see e.g. United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998); United States v. Yunis, 867 F.2d 617, 621-25 (D.C. Cir. 1989). In this case, upon consideration of the government’s classified CIPA motion, the Court signed the protective order. This portion of the Court’s file remains classified and under seal.

Meanwhile, on April 1, 2016 (which was the deadline for all discovery motions in this case), the defendant filed a Motion for a Bill of Particulars seeking additional information about the government’s evidence and its theory of prosecution. The government opposed the defendant’s motion, in large part because the government had already produced voluminous and organized discovery which had directed the defendant’s attention to the government’s key

¹ Section 4 provides, in pertinent part, that a district court:

upon a sufficient showing may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The Court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone.

evidence. The court denied this motion in its entirety.

Thereafter, on April 19, 2016 (over two weeks after the discovery motion deadline), the defense sent a letter to the government requesting “notice and supplemental discovery of any surveillance techniques or searches that contributed to the government’s investigation of the defendant, including but not limited to” more than a dozen categories of surveillance techniques that exist under the law and today’s technology, ranging from classified surveillance pursuant to the Foreign Intelligence Surveillance Act (FISA), to GPS-tracking devices. In this letter, the defense claimed the government “has an obligation to provide notice and discovery concerning the surveillance it employed because, without that information, Ms. Thomas is unable to challenge the legality of the surveillance and the admissibility of evidence derived or obtained therefrom.” On May 5, 2016, the government responded with a lengthy letter explaining that Thomas was not – under any statute, rule, or judicial opinion – entitled to the information she requested because: (a) a defendant has no right to receive notice about the fact that the government chose to utilize a particular surveillance technique, when the government is not using (and thus a defendant may not seek to suppress) any evidence obtained from said surveillance technique; (b) when it comes to classified surveillance techniques, federal statutes strictly limit a defendant’s right to notice and discovery thereof; and (c) the government has fully complied with all criminal discovery rules and requirements. Def. Exhibit F.

On June 28, 2016, nearly two months after the aforementioned exchange of correspondence (and almost three months past the deadline for discovery motions), the defense filed a Motion for Notice and Discovery of Surveillance Used in the Government’s Investigation of the Defendant. In this motion, Thomas again seeks “to compel the government to provide

notice and discovery of surveillance it used to monitor Ms. Thomas's communications and activities, so that the defense has an adequate opportunity to challenge the lawfulness of the surveillance actually used in this case." Def. Mem. at 2. For the reasons set forth in the government's original letter response as well as below, this motion is without merit and should be denied.

B. Discussion

Thomas argues that she is entitled to notice and discovery of all surveillance techniques used by the government in this investigation, both classified and unclassified, so that she may challenge their lawfulness. Def. Mem. at 3. However, the defendant's argument entirely misunderstands the government's discovery obligation in criminal cases. As explained below, notice and discovery about the government's surveillance techniques is not required under the Federal Rules of Criminal Procedure. See Fed. R. Crim. P. 16 (limiting government's discovery obligation to specific categories of evidence). Nor do Brady or Giglio principles apply, because the government's decision to use a particular investigatory authority is neither material to guilt or punishment, nor exculpatory or impeaching. Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972). The Jencks Act (requiring production of prior witness statements) is also irrelevant.

In fact, the government's decision to use a particular surveillance technique is only discoverable if evidence gathered pursuant to that technique is being used by the government and therefore may be the subject of a defense suppression motion. As explained below, this is the case whether the surveillance is unclassified, see 18 U.S.C. § 3504 (notice regarding "sources of evidence" may be required when defendant claims "that evidence is inadmissible"), or classified,

see FISA, 50 U.S.C. §§ 1806 , 1825, 1845(c) (notice required only when government intends to enter into evidence or otherwise use or disclose evidence gathered pursuant to FISA).

In this case, all unclassified search warrants which Thomas has standing to suppress have already been produced, and therefore 18 U.S.C. § 3504 is satisfied. And the government is not and will not be using any evidence gathered pursuant to classified techniques, so Thomas's request for notice and discovery of classified surveillance techniques is moot. Therefore, Thomas's motion is entirely without merit and should be denied.

1. **Applicable Rules and Statutes Do Not Entitle Defendant to the Broad Notice and Discovery She Seeks**

Contrary to defendant's argument, there is no overarching governmental obligation to notify a defendant of all investigative techniques utilized in an investigation. Rather, discovery in criminal cases is limited to those categories outlined in Federal Rule of Criminal Procedure 16, "with some additional material being discoverable in accordance with statutory pronouncements and the due process clause of the constitution." United States v. Ramos, 27 F.3d 65, 68 (3d Cir. 1994). Generally, these other areas are limited to the Jencks Act and materials pursuant to Brady and Giglio. Id. Further, Federal Rule of Criminal Procedure 12(b)(4)(B) ("Notice of the Government's Intent to Use Evidence"), which addresses pre-suppression discovery requests like this, expressly limits pre-suppression discovery to those categories outlined in Rule 16. See Rule 12(b)(4)(B) ("defendant may, in order to have an opportunity to move to suppress evidence . . . request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under rule 16").

Further, courts have long espoused the principal that it is the government's obligation to determine whether information in its possession, custody, or control is subject to

discovery. See, e.g., United States v. Campa, 529 F.3d 980, 996 (11th Cir. 2008) (“Ordinarily, the government alone determines whether material in its possession must be turned over to a defendant.”). Thus, a defendant may not compel information merely to ensure the government is complying with its legal and ethical discovery obligations. See, e.g., United States v. Rivera, 198 F.R.D. 48 (W.D.N.Y. 1999) (denying defendant’s request for inspection of pen register, where defendant provides no reason to believe the device may have contravened his constitutional or statutory rights). Nor does a defendant have any “constitutional right to conduct [her] own search of the government’s files to argue relevance.” Pennsylvania v. Ritchie, 480 U.S. 39, 59 (1987).

Defendant nonetheless argues that complete notice and discovery is required in this case because this investigation likely involved surreptitious surveillance, and courts routinely require notice and discovery when surveillance is surreptitious (such as with wiretaps and sneak-a-peek entries). Def. Mem. at 26-28. However, none of the case examples cited by Thomas addresses classified surveillance techniques, and this is a critical distinction for two reasons. First, when it comes to classified information, there is a compelling need to protect it against disclosure. See CIA v. Sims, 471 U.S. 159, 175 (1985) (citing the government’s “compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service”) (quoting Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam)); accord Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) (“The [executive branch] has available intelligence services whose reports are not and ought not to be published to the world.”). Accordingly, federal courts have long recognized that “[i]t is not in the national interest for revelation of either the existence or the product of [foreign

intelligence operations and information] to extend beyond the narrowest limits compatible with the assurance that no injustice is done to the criminal defendant.” United States v. Lemonakis, 485 F.2d 941, 963 (D.C. Cir. 1973).

Second, unlike with the unclassified surveillance examples provided in Thomas’s motion, Congress has enacted very clear statutory criteria for the government’s notice obligations regarding classified investigative techniques. And, as set forth below, none of the notice obligations apply in this case:

- a. FISA Surveillance: When FISA surveillance is used, federal statute explicitly states that the government’s notice obligations apply only if the government (1) intends to enter into evidence or otherwise use or disclose (2) against an aggrieved person (3) in a trial, hearing or other proceeding (4) any information obtained or derived from (5) FISA. 50 U.S.C. §§ 1806 (electronic surveillance), 1825 (physical search), 1845(c) (pen register or trap and trace). If the statutory criteria for notice identified above were satisfied in this case, the United States would have provided notice to the defendant and the Court that the United States intended to use against the defendant information obtained or derived from FISA. No such notice has been provided to the defendant or Court because the statutory requirements have not been satisfied.
- b. Surveillance Under Executive Order 12333: Thomas claims she is entitled to notice of any classified surveillance conducted under Executive Order 12333, but this Executive Order creates no new notice or discovery

procedures outside of FISA. United States v. Marzook, 435 F. Supp.2d 778 (N.D. Ill. 2006) (FISA now governs the process for obtaining intelligence searches); United Presbyterian Church v. Reagan, 557 F. Supp. 61 (D.D.C. 1982) (denying request for “production of all documents which described the manner in which the Federal Bureau of Investigation and the Central Intelligence Agency would carry out their responsibilities under Executive Order 12333, and all documents relating to which plaintiffs had been or would be ‘targeted’ and what information on them had been developed. Such a request is a ‘fishing expedition’ of the most obvious kind . . .”). Thus, the procedures laid out in FISA, created by Congress and set forth in clear statutory language discussed above, continue to control.

- c. Collection of Third-Party Records Pursuant to FISA and/or via National Security Letters (NSLs): Thomas also argues that she is entitled to notice and discovery of any collection of third-party business records pursuant to either Section 215 of the Patriot Act (which amended portions of FISA), or through the use of National Security Letters (NSLs). Both procedures provide the government with an ability, in national security investigations, to obtain third-party business records in a way similar to grand jury subpoenas. And just like with grand jury subpoenas, there is no requirement to provide a defendant with notice or discovery of the process used. United States v. Miller, 425 U.S. 435, 444 (1976) (the “issuance of a

subpoena to a third party to obtain the records of that party does not violate the rights of a defendant”); see also United States v. Amawi, 531 F. Supp.2d 823 (N.D. Oh. 2008) (denying defendant’s discovery request for NSLs in order to determine whether the government violated constitutional rights; NSLs are not discoverable); 50 U.S.C. §§ 1861-62 (no notice requirement within Section 215). Nor is there any suppression remedy available even if the government had committed some statutory violation, since applicable statutes provides for none, and because Thomas would lack standing to contest the admission of records collected from third parties. See, e.g Miller, 425 U.S. at 444.

The defendant attempts to sidestep all of the above by claiming that the U.S. Constitution and 18 U.S.C. § 3504 entitle her to full notice and discovery of all surveillance techniques, because “[t]he only way to vindicate a criminal defendant’s right to suppress illegally acquired evidence is through notice.” Def. Mem. at 26 (Rules 12, 16), 31 (§ 3504). It is true that, under 18 U.S.C. § 3504, an “aggrieved” party does have the right to receive notification of surveillance whenever a colorable claim is made that “evidence is inadmissible” because it was obtained via “any electronic, mechanical, or other device . . . in violation of the Constitution or laws.” 18 U.S.C. § 3504. But this means that § 3504 is limited to notice of surveillance which captured evidence about which there may be an admissibility dispute. This is reminiscent of the FISA notice requirement, which is also limited to surveillance which captured evidence that the government intends to admit in court. 50 U.S.C. §§ 1806, 1825, 1845(c). And here lies the fatal flaw in Thomas’s argument – her demand for notice and discovery of surveillance techniques has

no merit to the extent it addresses techniques from which the government is not using any evidence. For in such instances, there is no possible suppression motion available to the defendant, because there would be nothing to suppress. In other words, such discovery arguments would be entirely moot.

In this case, all unclassified search warrants authorizing the government's searches of Thomas's hard drives, home, and various online accounts have already been produced in discovery, which fully satisfies the government's discovery obligations under all applicable rules and § 3504.² And the government does not intend to introduce a single piece of evidence in this

² Thomas's motion alleges that the government has failed to produce certain critical pieces of evidence, but these allegations are factually incorrect.

a. Thomas points to one search warrant affidavit in which the government explains that it relied on "other lawful search warrants" to obtain her Facebook communications. Def. Mem. at 5. This is a reference to warrants executed on third-party Facebook accounts whose users were communicating with Thomas. All of these relevant search warrant returns were in fact produced to Thomas during discovery. However, Thomas has no standing to challenge nor suppress these returns because the accounts belonged to third-parties, not Thomas. Thus, this request is moot because it addresses third-party records which she has no standing to suppress. Miller, 425 U.S. at 443 ("Fourth Amendment does not prohibit the obtaining of information revealed to a third party"); United States v. Padilla, 113 S. Ct. 1936 (1993) (co-conspirator relationship does not broaden an individual's Fourth Amendment standing to challenge a search and seizure).

b. Thomas claims that the government has not provided any information revealing how the government obtained her unique IP address. Def. Mot. at 5. This is not accurate, for such documents were obtained by way of a Grand Jury subpoena to Thomas's telecommunications provider, then confirmed by Facebook and her other social media hosts, and all such documents were produced to Thomas as part of discovery.

c. Thomas refers to a statement made at her probable cause hearing that the government used "other investigative tools" to collect her personal information and monitor her social media accounts. Def. Mem. at 6. This comment – made in open court – was a general reference to all unclassified tools used to investigate Thomas. And as stated above, full unclassified discovery has already been produced, revealing the use of several investigative tools (including subpoenas, search warrants, and witness interviews).

case that was gathered pursuant to classified surveillance techniques, which means Thomas is not entitled to notice or discovery of any classified processes.

In sum, no court has ever adopted the discovery paradigm set forth by the defense, requiring the government to give an accounting of every surveillance technique used in its case, classified and unclassified, and regardless of its relationship to any potential suppression motion. And more importantly, no court has ever held that notice of FISA activity must be provided outside of FISA's statutory scheme.

2. **The Government Is Not Improperly Hiding Aspects of This Investigation**

Throughout her motion, Thomas cites various news articles claiming that the government routinely conducts classified surveillance in violation of people's constitutional rights. This material is a red herring, for Thomas's incendiary allegations have no relevance to

d. Thomas claims a "possible violation" of the Constitution may have occurred, because Homeland Security Investigations (HSI) agents participate in the joint task force that investigated Thomas, and because HSI agents "routinely monitor, retain, and analyze social media posts of U.S. persons in possible violation of the First and Fourth Amendments." Def. Mem. at 6. This generalized and speculative argument about conduct in other investigations is a red herring, because all unclassified discoverable information specific to this case has already been produced, and any classified information has already been considered by this Court under CIPA.

e. Thomas claims that the government must have used foreign intelligence tools in this investigation. Def. Mem. at 7. However, as set forth above in the body of this response, any notice requirement stemming from the use of such classified tools is delineated by statute, and not applicable here.

f. Finally, Thomas argues that the government "has an obligation to disclose information that it expressly relied upon in seeking its Rule 41 search warrants." Def. Mem. at 34. However, as set forth above, all affidavits supporting warrants to search Thomas's accounts, home, and electronics have already been produced to her. Thus, the government is not withholding any discoverable information.

the government's discovery obligations and conduct in this case. As explained above, the government will not be seeking to introduce any evidence in this case that was gathered via classified techniques. Thus, Thomas's arguments seeking notice and disclosure of classified surveillance techniques are all moot.

In addition, and perhaps even more importantly, the government is not hiding any classified processes in this case, but rather submitted a CIPA Section 4 motion which this Court reviewed and granted. In fact, Thomas's motion entirely fails to recognize that the CIPA processes used by the government here exist precisely so courts may ensure that defendants' constitutional rights are protected when classified information is involved. United States v. Pappas, 94 F.3d 795, 799 (2d Cir. 1996) (CIPA's fundamental purpose is to "harmonize a defendant's right to obtain and present exculpatory material [at] trial and the government's right to protect classified material in the national interest").

As stated above, CIPA Section 4 expressly allows the United States to request that the court review, ex parte and in camera, classified information to determine whether it is discoverable under Rule 16, Brady v. Maryland, 373 U.S. 83 (1963), Giglio v. United States, 405 U.S. 150 (1972), or the Jencks Act, and to protect such classified information from disclosure through various means if it is discoverable. See United States v. Libby, 429 F. Supp. 2d 18, 22 (D.D.C. Apr. 5, 2006) (amended by United States v. Libby, 429 F. Supp. 2d 46, 47 (D.D.C. May 3, 2006)); also United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261-62 (9th Cir. 1998); Rezaq, 134 F.3d at 1142; Yunis, 867 F.2d at 619-25; United States v. Pringle, 751 F.2d 419, 427-28 (1st Cir. 1984); Kasi v. Angelone, 200 F. Supp. 2d 585, 596 n.6 (E.D. Va. 2002). For example, the government may request that the Court deny discovery of a classified document in

its entirety pursuant to Section 4 because it is not discoverable under the relevant legal standard. Libby, 429 F. Supp. at 48. Alternatively, the government may file a motion under Section 4 to delete specific classified information from a document that either the government or the Court has deemed discoverable, or to substitute an unclassified summary or admission in the place of the document. Id. at 47. If the court determines that the disputed document is not subject to discovery or, if it is, permits deletion or substitution³ of the classified information, then the entire text of any ex parte in camera pleadings shall be sealed and preserved in the court's record to be made available to the appellate court in the event of an appeal. 18 U.S.C. App. III § 4; see also United States v. Aref, No. 04-CR-402, 2006 WL 1877142, at *2 (S.D.N.Y. July 6, 2006).

Thus, Thomas's alleged concern over the government's "record of withholding notice and discovery of surveillance" is misplaced here. Def. Mem. at 8-9, 20. For in this case, the Court decided the extent of the government's classified obligations via a CIPA Section 4 motion.

C. Motion to Seal

In deference to the defendant's request that her underlying Motion be filed under seal, and in the interest of caution, the government requests that this Response be filed under seal as well.

D. Conclusion

In this motion, Thomas questions the legality of various classified investigative

³ Thomas's claim that the government routinely and unlawfully avoids scrutiny of its classified techniques by hiding behind "parallel construction" (obtaining via unclassified means certain communications which the government had already obtained via classified means) is incorrect and reveals a lack of understanding of CIPA. In fact, CIPA expressly permits a Court to order the government to substitute an unclassified version of evidence for a classified version where appropriate. Libby, 429 F. Supp. at 47.

practices – such as the “NSA’s bulk call-records program,” the “StellarWind” program, and “FAA Section 702 surveillance” – based on descriptions contained in various news articles. Def. Mem. at 9-11. However, such practices have nothing to do with the government’s discovery obligations in this case, nor is this motion an appropriate tool to raise such a global challenge to classified investigative tools. As set forth above, the specific facts of this case simply do not entitle Thomas to the notice and discovery she seeks.

That said, the government understands and has fully complied with its discovery obligations under the Federal Rules of Criminal Procedure, the Jencks Act, Brady v. Maryland, 373 U.S. 83 (1963), and Giglio v. United States, 405 U.S. 150 (1972), and all other authorities. The government further understands that its obligation to produce discovery is a continuing one, and it will continue to provide discovery as required and appropriate.

WHEREFORE, the government respectfully submits that the Defendant’s Motion for Notice and Discovery of Surveillance Used in the Government’s Investigation of the Defendant be DENIED in its entirety.

ZANE DAVID MEMEGER
UNITED STATES ATTORNEY


JENNIFER ARBITTIER WILLIAMS
Assistant United States Attorney

PAUL CASEY
Trial Attorney
Counterterrorism Section
U.S. Department of Justice

CERTIFICATE OF SERVICE

I certify that a copy of the Government's Response in Opposition to Defendant's Motion for Notice and Discovery of Surveillance Used in the Government's Investigation of the Defendant was served by e-mail on the following defense counsel:

Kathleen M. Gaughan, Esquire
Elizabeth L. Toplin, Esquire
Defender Association Of Philadelphia
Federal Court Division
The Curtis Center Building
601 Walnut Street, Suite 540 West
Independence Square West
Philadelphia, PA 19106


JENNIFER ARBITTIER WILLIAMS
Assistant United States Attorney

Date: July 19, 2016